

Relating p -adic eigenvalues and the local Smith normal form

Mustafa Elsheikh, Mark Giesbrecht
 melsheik@uwaterloo.ca, mwg@uwaterloo.ca
 Cheriton School of Computer Science,
 University of Waterloo, Canada

May 8, 2015

Abstract

Conditions are established under which the p -adic valuations of the invariant factors (diagonal entries of the Smith form) of an integer matrix are equal to the p -adic valuations of the eigenvalues. It is then shown that this correspondence is the typical case for “most” matrices; density counts are given for when this property holds, as well as easy transformations to this typical case.

Keywords

Integer matrices, p -adic numbers, eigenvalues, Smith normal form

AMS Subject Classification

15A36, 15A18, 15A21

1 Introduction

Recall that any matrix $A \in \mathbb{Z}^{n \times n}$ of rank r can be written as $A = PSQ$ where $P, Q \in \mathbb{Z}^{n \times n}$ are unimodular matrices (i.e., whose inverses are also in $\mathbb{Z}^{n \times n}$) and $S = \text{diag}(s_1, \dots, s_r, 0, \dots, 0)$ is the *Smith normal form* (SNF)

of A , where $s_1, \dots, s_r \in \mathbb{Z}$ are A 's *invariant factors*, and $s_1 \mid s_2 \mid \dots \mid s_r$. Alternatively, if we define the i th *determinantal divisor* Δ_i of A as the GCD of all $i \times i$ minors of A , then Δ_{i-1} divides Δ_i and $s_1 = \Delta_1$ and $s_i = \Delta_i / \Delta_{i-1}$ for $2 \leq i \leq r$. See (Newman, 1972) for a full treatment of this theory.

A priori the invariant factors of a matrix and the *eigenvalues* of a matrix would seem to be rather different invariants, the former related to the \mathbb{Z} -lattice structure of A and the latter to the geometry of the linear map. We show that, in fact, they are “usually” in one to one correspondence with respect to their p -adic valuations at a prime p . We demonstrate a simple sufficient condition under which this holds for any integer matrix, and provide bounds on the density of matrices for which it holds. The list of powers of p in the invariant factors are often referred to as the *local Smith form at p* by some authors (Gerstein, 1977; Dumas et al., 2001; Wilkening and Yu, 2011; Elsheikh et al., 2012).

Throughout we will work in the ring of p -adic integers $\mathbb{Z}_p \supseteq \mathbb{Z}$, the p -adic completion of \mathbb{Z} , and its quotient field $\mathbb{Q}_p \supseteq \mathbb{Q}$, the p -adic numbers. See (Koblitz, 1984) or (Gouvêa, 1997) for an introduction. Let $v_p(a) \in \mathbb{N} \cup \{\infty\}$ be the p -adic order or p -adic valuation of any $a \in \mathbb{Z}_p$, the number of times p divides a exactly, where $v_p(0) = \infty$. The valuation can be extended to \mathbb{Q}_p by letting $v_p(a/b) = v_p(a) - v_p(b)$ for $a, b \in \mathbb{Z}_p$.

Example 1. Consider the matrix

$$A = \begin{pmatrix} 3 & -1 & 3 \\ 9 & -10 & 0 \\ 3 & 0 & 3 \end{pmatrix} = \overbrace{\begin{pmatrix} 1 & -1 & 0 \\ 1 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}}^U \overbrace{\begin{pmatrix} 1 & & \\ & 3 & \\ & & 9 \end{pmatrix}}^S \overbrace{\begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & -1 \\ 1 & -1 & 0 \end{pmatrix}}^V,$$

for unimodular U, V and Smith form S of A . Now consider the eigenvalues of A , which are roots of the characteristic polynomial

$$f = \det(xI - A) = x^3 + 4x^2 - 51x - 27 \in \mathbb{Z}[x].$$

We find it has three distinct roots in \mathbb{Z}_3 :

$$\begin{aligned} \lambda_1 &= -1 - 3^3 - 3^4 - 3^5 - 3^6 - 3^8 + 3^9 + O(3^{10}), \\ \lambda_2 &= -3 - 3^2 - 3^3 - 3^4 + 3^6 - 3^8 - 3^9 + O(3^{10}), \\ \lambda_3 &= 3^2 - 3^3 - 3^5 + 3^6 - 3^8 + 3^9 + O(3^{10}). \end{aligned}$$

In this example we see that $v_3(\lambda_1) = 0$, $v_3(\lambda_2) = 1$ and $v_3(\lambda_3) = 2$. Recalling that the Smith form of A above is $S = \text{diag}(1, 3, 3^2)$, we see that the diagonal entries of the Smith form have precisely the same p -adic valuations as the eigenvalues of A . \square

The eigenvalues of A are roots of the characteristic polynomial, which has a natural image in $\mathbb{Z}_p[x]$ since \mathbb{Z}_p contains \mathbb{Z} . Thus, the eigenvalues of A can naturally be viewed as p -adic algebraic integers in a finite-degree algebraic extension field K_p over \mathbb{Q}_p (Gouvêa, 1997, Proposition 5.4.5 (v)).

In order to show the correspondence between the eigenvalues and the invariant factors, we need to extend the definition of the valuation v_p to the eigenvalues (more generally, to the elements of K_p). If an element $a \in K_p$ has a minimal polynomial $x^{d_a} + a_{d_a-1}x^{d_a-1} + \dots + a_0 \in \mathbb{Q}_p[x]$, then the valuation is uniquely given by $v_p(a) = (1/d_a)v_p(a_0)$. See (Koblitz, 1984, §3, pp. 66). The image of the extended v_p is \mathbb{Q} , and its restriction to \mathbb{Q}_p agrees with the earlier definition of v_p on \mathbb{Q}_p . The valuation of a non-zero eigenvalue $v_p(\lambda_i)$ is independent of the choice of K_p , since it only depends on the minimal polynomial of λ_i over \mathbb{Q}_p . In particular, the set of minimal polynomials of the non-zero eigenvalues is precisely the set of irreducible factors of the characteristic polynomial of the matrix over \mathbb{Q}_p regardless of the field extension. Therefore, $v_p(\lambda_1), \dots, v_p(\lambda_n)$ are invariants of the matrix over \mathbb{Q}_p , and independent of the p -adic extension chosen to contain the eigenvalues.

In light of the above, we will treat integer matrices and their eigenvalues as being naturally embedded in \mathbb{Z}_p , \mathbb{Q}_p or K_p as appropriate, under the p -adic valuation v_p .

It should be noted that the correspondence between the valuations of the eigenvalues and the invariant factors does not hold for all matrices.

Example 2. *Let*

$$A = \begin{pmatrix} 37 & 192 & 180 & 369 \\ 55 & 268 & 198 & 531 \\ 163 & 758 & 442 & 1539 \\ 198 & 908 & 486 & 1858 \end{pmatrix},$$

which has the Smith form decomposition:

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 2 & & \\ & & 2 & \\ & & & 4 \end{pmatrix} \begin{pmatrix} 163 & 758 & 442 & 1539 \\ 99 & 454 & 243 & 929 \\ -54 & -245 & -122 & -504 \\ -54 & -246 & -126 & -505 \end{pmatrix}.$$

The characteristic polynomial of A is

$$f = x^4 - 2605x^3 + 39504x^2 + 40952x + 16 \in \mathbb{Z}[x]$$

which factors over \mathbb{Q}_2 into

$$x + (1 + 2^2 + 2^3 + O(2^5)) \in \mathbb{Z}_2[x]$$

and the irreducible factor

$$x^3 + (2^3 + O(2^5))x^2 + (2^3 + 2^4 + O(2^5))x + (2^4 + O(2^5)) \in \mathbb{Z}_2[x].$$

Using Newton slopes (see Fact 1 below) we find that the 2-adic valuations of the roots of the second factor are $[4/3, 4/3, 4/3]$. Thus, the 2-adic valuations of the invariant factors of A are $[0, 1, 1, 2]$, while the 2-adic valuations of the eigenvalues of A are $[0, 4/3, 4/3, 4/3]$. The p -adic valuations of the eigenvalues and the invariant factors are therefore not in 1-1 correspondence. \square

In the remainder of this paper we explore the conditions under which this correspondence between the p -adic valuation of invariant factors and eigenvalues occurs, and show that it is, in fact, the “typical” case, i.e., it holds for “most” matrices.

1.1 Main Results

We first define two important matrix properties for our purposes.

Definition 1. Let $A \in \mathbb{Z}^{n \times n}$ be of rank r and p be any prime. Assume

- (i) A has Smith form $S = \text{diag}(s_1, \dots, s_r, 0, \dots, 0)$ over \mathbb{Z} , so that $\Delta_i = s_1 \cdots s_i$ is the i th determinantal divisor of A , for $1 \leq i \leq r$;
- (ii) A has non-zero eigenvalues (with multiplicity) $\lambda_1, \dots, \lambda_r$ in a finite-degree extension K_p over \mathbb{Q}_p , and assume that $v_p(\lambda_1) \leq \dots \leq v_p(\lambda_r)$;
- (iii) A has characteristic polynomial $f = x^n + f_1x^{n-1} + \dots + f_rx^{n-r} \in \mathbb{Z}[x]$ (note the reversed indexing).

We say A is p -characterized if and only if $v_p(f_i) = v_p(\Delta_i)$ for all $i \in [1, r]$. We say A is p -correspondent if and only if $v_p(s_i) = v_p(\lambda_i)$ for all $i \in [1, r]$.

Note that if A is p -correspondent, then the valuations of the eigenvalues are non-negative integers (since $v_p(s_i) \geq 0$). Our main goal is to study the notion of p -correspondence; that is the relationship between the spectrum and the invariant factors. The notion of p -characterization is an auxiliary definition used throughout our proofs. The following theorem gives the relationship between a matrix being p -correspondent and being p -characterized; the proof is in Section 2.

Theorem 1. *Let $A \in \mathbb{Z}^{n \times n}$ and p be a prime. If A is p -characterized then A is p -correspondent.*

Of course, not all matrices are p -correspondent at any particular prime p , but it is generally possible to transform a matrix to a p -correspondent one. We offer the following two simple lemmas in this regard, the proofs of which are in Section 2.

Lemma 1. *Let $A \in \mathbb{Z}^{n \times n}$ and p be any prime. There exists an equivalence transformation $P, Q \in \text{GL}_n(\mathbb{Z})$ such that PAQ is p -correspondent.*

Lemma 2. *Let $A \in \mathbb{Z}^{n \times n}$ be non-singular, p be any prime. There exists a similarity transformation U with entries in an extension K_p over \mathbb{Q}_p such that $U^{-1}AU$ is p -correspondent.*

In Section 3 we establish that “most” matrices are p -correspondent. We will consider the density in each equivalence class defined by a given Smith form S . The following definition helps capture this.

Definition 2. *Fix a prime p , positive integers m, n , and integers $0 \leq e_1 \leq e_2 \leq \dots \leq e_n$. Let $S = \text{diag}(p^{e_1}, \dots, p^{e_n}) \in \mathbb{Z}^{n \times n}$. Define $\mathfrak{S}_S^m \subseteq \mathbb{Z}^{n \times n}$ as the set of integer matrices with entries from $[0, p^m)$ whose Smith form $\text{diag}(s_1, \dots, s_n)$ satisfies $v_p(s_i) = e_i$ for all $i \in [1, n]$.*

Our main result is then as follows.

Theorem 2. *Let n be a positive integer, $\epsilon > 0$, and p any prime greater than $16(n^2 + 3n)/\epsilon$. Fix a set of integers $0 \leq e_1 \leq e_2 \leq \dots \leq e_n$ and let $m \geq e_1 + \dots + e_n + 1$ and $S = \text{diag}(p^{e_1}, \dots, p^{e_n}) \in \mathbb{Z}^{n \times n}$. Then the number of matrices in \mathfrak{S}_S^m which are p -characterized and hence p -correspondent is at least $(1 - \epsilon) \cdot |\mathfrak{S}_S^m|$.*

1.2 Previous Work

Newman and Thompson (1991), Section 8, study the relationship between eigenvalues and invariant factors of matrices over rings of algebraic integers. Their results are concerned with products of eigenvalues rather than individual eigenvalues (or subsets thereof). For any square matrix over a ring R of algebraic integers with invariant factors s_1, \dots, s_n and eigenvalues $\lambda_1, \dots, \lambda_n$ (in some extension¹ \bar{R} of R), they prove (in Theorem 6) that for all $k \in \{1, \dots, n\}$ and all indexing sets $I \subseteq \{1, \dots, n\}$, $|I| = k$,

$$s_1 s_2 \cdots s_k \mid \prod_{i \in I} \lambda_i.$$

where divisibility is taken over \bar{R} .

Rushanan (1995) studied the Smith form and spectrum of non-singular matrices with integer entries. He established divisibility relations between the largest invariant factor s_n and the product of all eigenvalues. Recently, the connection between the eigenvalues and Smith form has also been studied by Kirkland (2007) for integer matrices with integer eigenvalues arising from the Laplacian of graphs, and by Lorenzini (2008) for Laplacian matrices of rank $n - 1$.

2 Establishing p -correspondence

We proceed to prove Theorem 1, that all p -characterized matrices are p -correspondent. First recall that the coefficients of the characteristic polynomial $f = x^n + \sum_{1 \leq i \leq n} f_i x^{n-i} \in \mathbb{Z}[x]$ of a matrix $A \in \mathbb{Z}^{n \times n}$ are related to the minors of A . For $1 \leq i \leq n$, let \mathcal{C}_i^n denote the set of all i -tuples of integers of the form $t = (t_1, \dots, t_i)$ where $1 \leq t_1 < \dots < t_i \leq n$. For $\sigma, \tau \in \mathcal{C}_i^n$, let $A_{\sigma, \tau}^{(i)}$ denote the determinant of the $i \times i$ submatrix selected by rows $\sigma_1, \dots, \sigma_i$ and columns τ_1, \dots, τ_i ; this is the *minor* of A selected by σ and τ . It is well-known and easily derived that, for all $1 \leq i \leq n$,

$$f_i = (-1)^i \sum_{\sigma \in \mathcal{C}_i^n} A_{\sigma, \sigma}^{(i)}. \quad (2.1)$$

¹ As stated in (Newman and Thompson, 1991, Section 2) \bar{R} is taken to be a ring of algebraic integers which contains R such that every ideal generated within R becomes principal within \bar{R} .

Since Δ_i divides all $i \times i$ minors, we have $\Delta_i \mid f_i$, i.e., $v_p(f_i) \geq v_p(\Delta_i)$. Moreover, if A has rank r we have $f_{r+1} = f_{r+2} = \dots = f_n = 0$.

We will also require the so-called Newton polygon of the characteristic polynomial of A . For a polynomial $f = x^n + \sum_{1 \leq i \leq n} f_i x^{n-i} \in \mathbb{Z}_p[x]$, the *Newton polygon* of f , denoted by $\mathbf{NP}(f)$, is the lower convex hull of the following points in \mathbb{R}^2 : $\{(0, 0), (1, v_p(f_1)), \dots, (n, v_p(f_n))\}$ (we omit $(i, v_p(f_i))$ whenever $f_i = 0$). This hull is represented by a list of points $(x_1, y_1), \dots, (x_k, y_k) \in \mathbb{R}^2$ with $x_1 < x_2 < \dots < x_k$. For each segment of $\mathbf{NP}(f)$ connecting two adjacent points (x_{i-1}, y_{i-1}) and (x_i, y_i) , the *slope* of the segment is $m_i = (y_i - y_{i-1})/(x_i - x_{i-1})$ and the *length* of the segment is the length of its projection onto the x -axis, taken as $\ell_i = x_i - x_{i-1}$. An important use of this is the following.

Fact 1 (See [Koblitz \(1984\)](#), §IV.3, Lemma 4). *Let $f = x^n + f_1 x_{n-1} + \dots + f_n \in \mathbb{Z}_p[x]$ and $f_n \neq 0$. Let the roots of f (counting multiplicity) be $\lambda_1, \dots, \lambda_n$ in an extension K_p over \mathbb{Q}_p . If the Newton polygon of f has slopes m_1, \dots, m_k and lengths ℓ_1, \dots, ℓ_k as above, then for each $1 \leq j \leq k$, f has exactly ℓ_j roots $\lambda \in K_p$ whose valuation $v_p(\lambda) = m_j$.*

We now have all the tools to prove Theorem 1.

Theorem 1. *Let $A \in \mathbb{Z}^{n \times n}$ and p a prime. If A is p -characterized then A is p -correspondent.*

Proof. Assume that A is p -characterized with rank r and characteristic polynomial $f = \sum_{0 \leq i \leq r} f_i x^{n-i} \in \mathbb{Z}[x]$, and A has Smith form $S = \text{diag}(s_1, \dots, s_r, 0, \dots, 0) \in \mathbb{Z}^{n \times n}$. Also, assume that the p -adic valuations of the invariant factors s_1, \dots, s_r have multiplicities r_0, \dots, r_{e-1} as follows:

$$(v_p(s_1), \dots, v_p(s_r)) = (\underbrace{0, \dots, 0}_{r_0}, \underbrace{1, \dots, 1}_{r_1}, \dots, \underbrace{e-1, \dots, e-1}_{r_{e-1}}),$$

where $e = v_p(s_r) + 1$. Since A is p -characterized, by definition we have for $1 \leq i \leq r$ that

$$v_p(f_i) = v_p(\Delta_i) = \sum_{1 \leq j \leq i} v_p(s_j),$$

for all $1 \leq i \leq r$. For notational convenience, define m_i as

$$m_i = v_p(\Delta_{r_0+r_1+\dots+r_i}) = r_1 + 2r_2 + \dots + i \cdot r_i.$$

Grouping the non-zero coefficients of f by p -adic valuation we then have

$$\begin{aligned} & (v_p(f_1), \dots, v_p(f_r)) \\ &= \left(\underbrace{0, \dots, 0}_{r_0}, \underbrace{1, 2, 3, \dots, r_1}_{r_1}, \underbrace{m_1 + 2, m_1 + 4, \dots, m_1 + 2r_2}_{r_2}, \right. \\ & \quad \left. \dots, \underbrace{m_{e-2} + (e-1), m_{e-2} + 2(e-1), \dots, m_{e-2} + r_{e-1}(e-1)}_{r_{e-1}} \right). \end{aligned}$$

$\text{NP}(f)$ is easily seen to consist of e segments, where segment i has slope i , and length r_i , for $0 \leq i < e$ (a segment i may have length 0 if $r_i = 0$). Thus, by Fact 1, f has r_i roots λ with $v_p(\lambda) = i$. This accounts for all the non-zero roots of f , since $r_0 + r_1 + \dots + r_{e-1} = \text{rank}(A)$. Since these roots are the non-zero eigenvalues of A , we immediately see that A is p -correspondent. \square

It should be noted that the converse of Theorem 1 is not necessarily true. The matrix in the following example is p -correspondent but not p -characterized.

Example 3. *The invariant factors of*

$$A = \begin{pmatrix} -20 & -2 & 81 & -388 \\ 18 & -6 & -84 & 375 \\ 7 & 34 & 3 & 41 \\ 13004 & -11695 & -64944 & 289315 \end{pmatrix},$$

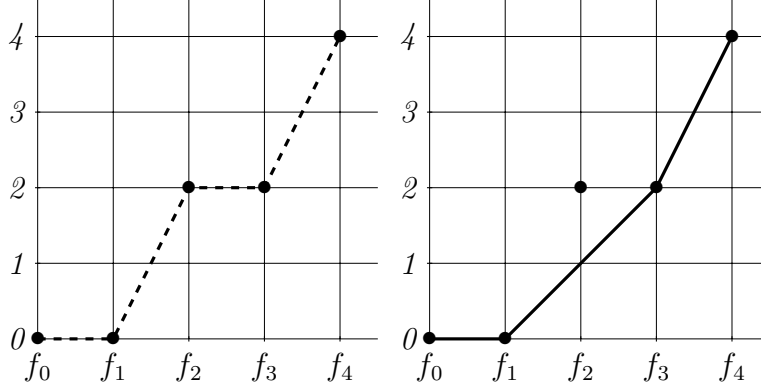
are $[1, 3, 3, 9]$, and the 3-adic eigenvalues are:

$$2 + O(3), \quad 2 \cdot 3 + O(3^3), \quad 3 + O(3^2), \quad 3^2 + O(3^3).$$

However, the 3-adic valuation of the determinantal divisors is $[0, 1, 2, 4]$ and the characteristic polynomial over $\mathbb{Z}_3[x]$ is:

$$x^4 + (1 + O(3))x^3 + (2 \cdot 3^2 + O(3^6))x^2 + (2 \cdot 3^2 + O(3^3))x + (3^4 + O(3)).$$

This is due to the fact that the Newton polygon of A is the convex hull of the segments defined by the coefficients of characteristic polynomial.



While the coefficients of the characteristic polynomial (points in left figure) do not correspond to the 3-adic valuations of the determinantal divisors, their lower convex cover (segments in right figure) corresponds to the 3-adic valuations of the invariant factors with slopes: 0, 1 (twice), and 2. \square

We now prove the two simple Lemmas 1 and 2, establishing p -correspondence under unimodular equivalence transformations and similarity.

Lemma 1. *Let $A \in \mathbb{Z}^{n \times n}$ and p be any prime. There exists an equivalence transformation $P, Q \in \text{GL}_n(\mathbb{Z})$ such that PAQ is p -correspondent.*

Proof. Simply choose $P, Q \in \text{GL}_n(\mathbb{Z})$ such that PAQ is in Smith normal form $S = \text{diag}(s_1, \dots, s_r, 0, \dots, 0)$. Then the eigenvalues of PAQ are s_1, \dots, s_r . \square

Lemma 2. *Let $A \in \mathbb{Z}^{n \times n}$ be non-singular, p be any prime. There exists a similarity transformation U with entries in an extension \mathbb{K}_p over \mathbb{Q}_p such that $U^{-1}AU$ is p -correspondent.*

Proof. Choose \mathbb{K}_p to be a splitting field of the minimal polynomial of A . It is well-known that A is similar to a matrix $J \in \mathbb{K}_p^{n \times n}$ in Jordan form. That is, there exists an invertible $W \in \mathbb{K}_p^{n \times n}$ such that $W^{-1}AW = \text{diag}(J_1, \dots, J_\ell)$ where

$$J_i = \begin{pmatrix} \mu_i & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \mu_i \end{pmatrix},$$

for some (not necessarily unique) eigenvalue $\mu_i \in \mathbb{K}_p$ of A , and J_i has dimensions $k_i \times k_i$. However, we can choose an alternative Jordan block \widehat{J}_i , similar to J_i , by applying the similarity transformation $\text{diag}(1, 1/\mu_i, \dots, 1/\mu_i^{k_i-1})$ to J_i to get

$$\widehat{J}_i = \begin{pmatrix} \mu_i & \mu_i & & \\ & \ddots & \ddots & \\ & & \ddots & \mu_i \\ & & & \mu_i \end{pmatrix}.$$

The Smith form of \widehat{J}_i can be obtained as follows. Subtract the first column from the second column. Then subtract the second column from the third, and so forth. The resulting matrix is $\text{diag}(\mu_i, \dots, \mu_i)$ which is in Smith normal form. Therefore \widehat{J}_i is p -correspondent.

Combining together the different Jordan blocks to form an alternative Jordan form \widehat{J} for A , we see that \widehat{J} is p -correspondent, and similar to A , as required. \square

Note that if A is singular, Lemma 2 may not hold. Consider for example

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

whose only eigenvalue is zero, with multiplicity two. This is also the case for any matrix similar to A . However, this matrix has rank one, and so one of the invariant factors must always be non-zero.

3 Density of p -characterized matrices

This section provides the proof for Theorem 2. We show that most matrices which are unimodularly equivalent to a matrix $A \in \mathbb{Z}^{n \times n}$, are p -characterized (and hence p -correspondent) when p is large compared to n . The main tool is the following.

In what follows, $\text{cont}(g)$ denotes the content of a polynomial g , that is, the GCD of the coefficients of g .

Lemma 3. *Let $A \in \mathbb{Z}^{n \times n}$ have rank r . Let \mathcal{U}, \mathcal{V} be $n \times n$ matrices whose $2n^2$ entries are algebraically independent indeterminates u_{ij} and v_{ij} respectively. Let g_k be the coefficient of x^{n-k} in the characteristic polynomial of $B = \mathcal{U}A\mathcal{V}$.*

Then for $k \in [1, r]$, g_k is a polynomial of total degree $2k$ and $\text{cont}(g_k)$ is Δ_k , the k th determinantal divisor of A .

Proof. Assume throughout that $k \leq r$. Using the Cauchy-Binet formula,

$$\begin{aligned} g_k &= (-1)^k \sum_{\sigma \in \mathcal{C}_k^n} B \begin{pmatrix} \sigma \\ \sigma \end{pmatrix} = (-1)^k \sum_{\sigma, \tau, \omega \in \mathcal{C}_k^n} \mathcal{U} \begin{pmatrix} \sigma \\ \tau \end{pmatrix} A \begin{pmatrix} \tau \\ \omega \end{pmatrix} \mathcal{V} \begin{pmatrix} \omega \\ \sigma \end{pmatrix} \\ &= (-1)^k \sum_{\tau, \omega \in \mathcal{C}_k^n} A \begin{pmatrix} \tau \\ \omega \end{pmatrix} \Upsilon_{\tau, \omega}, \quad \text{where} \quad \Upsilon_{\tau, \omega} = \sum_{\sigma \in \mathcal{C}_k^n} \mathcal{U} \begin{pmatrix} \sigma \\ \tau \end{pmatrix} \mathcal{V} \begin{pmatrix} \omega \\ \sigma \end{pmatrix}. \end{aligned} \quad (3.1)$$

We first show that $\Upsilon_{\tau, \omega}$ has content 1. By Leibniz's determinant expansion on the minor of \mathcal{U} selected by the first k rows, and the columns given by the indices in $\tau \in \mathcal{C}_k^n$, we have

$$\begin{aligned} \mathcal{U} \begin{pmatrix} (1, 2, \dots, k) \\ \tau \end{pmatrix} &= \sum_{\mu \in S_k} \text{sgn}(\mu) \prod_{1 \leq i \leq k} u_{\mu_i, \tau_i} \\ &= u_{1, \tau_1} u_{2, \tau_2} \cdots u_{k, \tau_k} + \sum_{\substack{\mu \in S_k \\ \mu \neq \text{id}}} \prod_{1 \leq i \leq k} \text{sgn}(\mu) u_{\mu_i, \tau_i}, \end{aligned}$$

where S_k is the symmetric group of permutations of k symbols, (μ_1, \dots, μ_k) is a permutation of $\{1, \dots, k\}$ and $\text{id} = (1, \dots, k)$ is the identity permutation. Similarly,

$$\mathcal{V} \begin{pmatrix} \omega \\ (1, \dots, k) \end{pmatrix} = v_{\omega_1, 1} v_{\omega_2, 2} \cdots v_{\omega_k, k} + \sum_{\substack{\mu \in S_k \\ \mu \neq \text{id}}} \prod_{1 \leq i \leq k} \text{sgn}(\mu) v_{\omega_i, \mu_i}.$$

We observe that $\mathcal{U} \begin{pmatrix} (1, 2, \dots, k) \\ \tau \end{pmatrix}$ contains the distinguished monomial $u_{1, \tau_1} \cdots u_{k, \tau_k}$ which is not found in any of the remaining terms of the expansion of $\mathcal{U} \begin{pmatrix} (1, \dots, k) \\ \tau \end{pmatrix}$ and hence has coefficient 1 (since each permutation μ is distinct), and is not found in the expansion of $\mathcal{U} \begin{pmatrix} \sigma' \\ \tau' \end{pmatrix}$ for any other $\sigma', \tau' \in \mathcal{C}_k^n$ (since the variables in the term allow us to identify the subsets σ' and τ'). Similarly, $\mathcal{V} \begin{pmatrix} \omega \\ (1, \dots, k) \end{pmatrix}$ contains the distinguished monomial $v_{\omega_1, 1} \cdots v_{\omega_k, k}$ with coefficient 1 which is not found in $\mathcal{V} \begin{pmatrix} \omega' \\ \sigma' \end{pmatrix}$ for any other $\omega', \sigma' \in \mathcal{C}_k^n$.

Thus, for every choice of τ, ω , the polynomial $\Upsilon_{\tau, \omega}$ has a monic distinguished term $u_{1, \tau_1} \cdots u_{k, \tau_k} v_{\omega_1, 1} \cdots v_{\omega_k, k}$ not appearing in $\Upsilon_{\tau', \omega'}$ for any other $\tau', \omega' \in \mathcal{C}_k^n$. Thus $\Upsilon_{\tau, \omega}$ is non-zero, has degree $2k$, and has content 1.

It follows immediately that g_k has degree $2k$ and content which is the GCD of all $A \begin{pmatrix} \tau \\ \omega \end{pmatrix}$, which is precisely Δ_k . \square

A related result is found in (Giesbrecht, 2001, Theorem 1.4). A similar technique is used in (Kaltofen and Saunders, 1991, Theorem 2), where a minor with symbolic entries is explicitly selected and shown to be lexicographically unique and hence the resulting polynomial, e.g. g_k , is shown to be non-zero.

The following lemma is used to count the number of matrices with a given property. While this result resembles the well-known Schwartz-Zippel lemma (Zippel, 1979; Schwartz, 1980), similar statements can be traced to earlier literature, for example in (Kasami et al., 1968).

Lemma 4. *Let p be a prime, $\ell \geq 1$ be an integer, and $g \in \mathbb{Z}[x_1, \dots, x_n]$ be a non-zero polynomial of total degree k . Then the number of points $\alpha = (\alpha_1, \dots, \alpha_n) \in [0, \ell p)^n$ for which $g(\alpha) \equiv 0 \pmod{p}$ is at most $\ell^n k p^{n-1}$.*

Proof. As a shorthand, we call $\alpha \in \mathbb{Z}^n$ a p -root if $f(\alpha) \equiv 0 \pmod{p}$. For $\ell = 1$ the statement of the lemma becomes exactly Corollary 1 of (Schwartz, 1980): the number of p -roots in the cube $[0, p)^n$ is at most $k p^{n-1}$.

Now assume $\ell > 1$. Every p -root $b \in [0, \ell p)^n$ can be written with component-wise Euclidean division as $(b_1, \dots, b_n) = (\alpha_1 + r_1 p, \dots, \alpha_n + r_n p) = \alpha + (r_1 p, \dots, r_n p)$ where $r_i \in [0, \ell - 1)$ and $\alpha = (\alpha_1, \dots, \alpha_n) \in [0, p)^n$. Then α must be a p -root because $b \equiv \alpha \pmod{p}$. Conversely if $\alpha = (\alpha_1, \dots, \alpha_n) \in [0, p)^n$ is a p -root, then $(\alpha_1 + r_1 p, \dots, \alpha_n + r_n p) \in [0, \ell p)^n$ is a p -root for all the ℓ^n possible values of $(r_1, \dots, r_n) \in [0, \ell)^n$. Thus there are at most $\ell^n \cdot k p^{n-1}$ p -roots in the cube $[0, \ell p)^n$. \square

Lemma 5. *Let $A \in \mathbb{Z}^{n \times n}$, $\epsilon > 0$, p a prime greater than $(n^2 + 3n)/\epsilon$, and N a non-zero integer divisible by p . The number of pairs of matrices (U, V) with entries from $[0, N)$ such that U and V are both non-singular modulo p , and that UAV is p -characterized, and hence p -correspondent, is at least $(1 - \epsilon)N^{2n^2}$.*

Proof. We show this count by associating each pair of matrices (U, V) with a point in $[0, N)^{2n^2}$ and then bounding the number of roots of a particular set of polynomials when evaluated in the cube $[0, N)^{2n^2}$.

First consider the product $\mathcal{U}A\mathcal{V}$ where \mathcal{U}, \mathcal{V} have symbolic independent indeterminates u_{ij} and v_{ij} for all $i, j \in [1, n]$. Let the characteristic polynomial of $\mathcal{U}A\mathcal{V}$ be

$$g = x^n + g_1 x^{n-1} + \dots + g_k x^{n-k} + \dots + g_n$$

Then each

$$\bar{g}_k = \frac{g_k}{\Delta_k(A)} \in \mathbb{Z}[u_{11}, u_{12}, \dots, v_{nn}]$$

is a polynomial in the entries of \mathcal{U}, \mathcal{V} with degree $2k$ and content 1 by Lemma 3

Each pair of matrices U, V in the lemma statement defines a point in $[0, N)^{2n^2}$; the entries of U, V define the values for the $2n^2$ variables u_{ij} and v_{ij} . The coefficients of the characteristic polynomial of each matrix UAV is obtained by evaluating the polynomials g_k at the point in $[0, N)^{2n^2}$ defined by (U, V) . Then using Lemma 4, we have $\bar{g}_k \equiv 0 \pmod{p}$ in at most $(N/p)^{2n^2} \cdot 2kp^{2n^2-1} = N^{2n^2} \cdot 2k/p$ points.

The determinant of \mathcal{U} (resp. \mathcal{V}) is a polynomial of degree n in all of the $2n^2$ variables u_{ij} (resp. v_{ij}), and hence $\det U \equiv 0 \pmod{p}$ in at most $(N/p)^{2n^2} np^{2n^2-1} = N^{2n^2} n/p$ points in the cube $[0, N)^{2n^2}$ by Lemma 4.

Thus the number of points in $[0, N)^{2n^2}$ for which $\det U \equiv 0 \pmod{p}$ or $\det V \equiv 0 \pmod{p}$, or that $\bar{g}_k \equiv 0 \pmod{p}$ for *some* $k \in [1, r]$ is at most

$$\frac{2nN^{2n^2}}{p} + \sum_{1 \leq k \leq r} \frac{2kN^{2n^2}}{p} = \frac{2nN^{2n^2}}{p} + \frac{r(r+1)N^{2n^2}}{p} \leq \frac{(n^2 + 3n)}{p} N^{2n^2} < \epsilon N^{2n^2}.$$

If all $\bar{g}_k \not\equiv 0 \pmod{p}$ for $k \in [1, r]$, then $v_p(\bar{g}_k) = 0$ and $v_p(g_k) = v_p(\Delta_k)$ for $k \in [1, r]$, so UAV is p -characterized, and hence p -correspondent. The number of pairs (U, V) for which this holds is then at least $N^{2n^2} - \epsilon N^{2n^2} = (1 - \epsilon)N^{2n^2}$. \square

Example 4. *Intuitively, Lemma 5 shows that most choices of the pairs (U, V) will result in UAV being p -correspondent. Consider the matrix:*

$$A = \begin{pmatrix} -48 & -83 & 91 & -497 \\ -407 & -666 & 637 & -3948 \\ 83 & 125 & -91 & 728 \\ -291 & -599 & 903 & -3717 \end{pmatrix},$$

A is not p -correspondent since its invariant factors are $[1, 7, 7, 49]$ and its 7-adic eigenvalues are (using the Sage computer algebra system):

$$\begin{aligned} &6 \cdot 7 + 7^2 + O(7^3), \\ &3 \cdot 7 + 3 \cdot 7^2 + O(7^3), \\ &1 \cdot 7 + 4 \cdot 7^2 + O(7^3), \\ &2 \cdot 7 + 3 \cdot 7^2 + O(7^3). \end{aligned}$$

Now consider a particular choice of $U, V \in \mathbb{Z}^{4 \times 4}$:

$$U = \begin{pmatrix} 6 & 1 & 0 & 20 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 2 \\ 1 & 3 & 0 & 1 \end{pmatrix}, \quad V = \begin{pmatrix} 1 & 1 & 1 & 17 \\ 0 & 0 & 3 & 2 \\ 0 & 5 & 1 & 3 \\ 1 & 0 & 9 & 56 \end{pmatrix}.$$

and let

$$\tilde{A} = UAV = \begin{pmatrix} -87785 & 89700 & -758134 & -4630434 \\ -4089 & 2813 & -35060 & -213813 \\ -12105 & 11261 & -104336 & -636989 \\ -17618 & 12965 & -151217 & -922413 \end{pmatrix}.$$

Using Sage we can verify that $\det U \not\equiv 0 \pmod{7}$, $\det V \not\equiv 0 \pmod{7}$, that the invariant factors of \tilde{A} are $[1, 7, 7, 2^{10} \cdot 7^2 \cdot 17]$ and that the 7-adic valuations of the eigenvalues of \tilde{A} are $[0, 1, 1, 2]$. As expected from Lemma 5, \tilde{A} is p -correspondent. \square

3.1 Density at large primes

To establish the density of p -correspondent matrices, we consider the set \mathfrak{S}_S^m of all matrices with a given a Smith form S and integer entries from $[0, p^m)$, and show that most matrices in this set are p -characterized.

We employ the notion of a Smith normal form over the ring $\mathbb{Z}/p^m\mathbb{Z}$. We choose $\{0, \dots, p^m - 1\}$ for representing the residue classes in this ring. For any non-zero $n \times n$ matrix A over the principal ideal ring $\mathbb{Z}/p^m\mathbb{Z}$, there exist two unimodular matrices $U, V \in \text{GL}_n(\mathbb{Z}/p^m\mathbb{Z})$ and a unique matrix $S_p = \text{diag}(p^{e_1}, \dots, p^{e_r}, 0, \dots, 0) \in (\mathbb{Z}/p^m\mathbb{Z})^{n \times n}$, for integers $0 \leq e_1 \leq \dots \leq e_r < m$, such that $A = US_pV$. A matrix $U \in \text{GL}_n(\mathbb{Z}/p^m\mathbb{Z})$ is unimodular if its inverse is also in $\text{GL}_n(\mathbb{Z}/p^m\mathbb{Z})$, or equivalently that its determinant is non-zero modulo p . We call S_p the Smith form of A over $\mathbb{Z}/p^m\mathbb{Z}$. Its existence and uniqueness follows from [Kaplansky \(1949\)²](#). If $\hat{A} \in \mathbb{Z}^{n \times n}$ is such that $\hat{A} \equiv A$

² Kaplansky uses the term *diagonal reduction* to denote the Smith form diagonalization, and *elementary divisor ring* to denote a ring over which every matrix admits a diagonal reduction (see §2, pp. 465). In the paragraph following Theorem 12.3 he concludes (on pp. 487) that every commutative principal ideal ring is an elementary divisor ring. In Theorem 9.3 he shows the uniqueness of the invariant factors (up to associates) by establishing an equivalent uniqueness result for modules rather than matrices. See his argument on

$(\text{mod } p^m)$, and \hat{A} has integer Smith form $\text{diag}(s_1, \dots, s_{\hat{r}}, 0, \dots, 0) \in \mathbb{Z}^{n \times n}$ then $r \leq \hat{r}$ and $e_i = v_p(s_i)$ for $1 \leq i \leq r$.

The following lemma relates the construction UAV in Lemma 5 to integer matrices with prescribed p -adic valuations on their invariant factors.

For any integer a and any prime power p^m , we use $a \text{ rem } p^m$ to denote the unique, non-negative, integer $r < p^m$ such that $a = qp^m + r$ for some integer q . We extend the “ $\text{rem } p^m$ ” operator to vectors and matrices using element-wise application. Note that “ $\text{rem } p^m$ ” operator is distinct from the “ $\text{mod } p^m$ ” equivalence relation; for example, $(a + b) \text{ rem } p^m \neq (a \text{ rem } p^m) + (b \text{ rem } p^m)$ in general.

Lemma 6. *Fix an integer n , a prime p , and integers $0 \leq e_1 \leq \dots \leq e_n < \infty$, and let $m > e_1 + \dots + e_n$. Let $S = \text{diag}(p^{e_1}, \dots, p^{e_n})$ and $\mathfrak{S}_S^m \subseteq \mathbb{Z}^{n \times n}$ as in Definition 2. Fix any $A \in \mathfrak{S}_S^m$. Let $L, R \in \mathbb{Z}^{n \times n}$ be any integer matrices satisfying $A = (LSR) \text{ rem } p^m$. Then $v_p(\det L) = v_p(\det R) = 0$, and hence L, R are both invertible modulo p^m .*

Proof. If $A = (LSR) \text{ rem } p^m$ then there exists an integer matrix Q (whose entries are the element-wise quotients of the Euclidean division) such that $A + p^m Q = LSR$. Taking the determinants of both sides, we have

$$\det(A + p^m Q) = \det(L) \det(S) \det(R).$$

Both sides are (products of) determinants, and hence polynomials in the matrix entries, and projecting modulo p^m we get

$$\det(A) \equiv \det(L) \det(S) \det(R) \pmod{p^m},$$

or equivalently

$$\det(A) + p^m q = \det(L) \det(S) \det(R),$$

for some $q \in \mathbb{Z}$.

Since $A \in \mathfrak{S}_S^m$ we know that $v_p(\det(A)) = v_p(\det(S))$, and moreover, $0 \leq v_p(\det(A)) < m$ by the conditions of the lemma. Thus $v_p(\det(A) + p^m q) = v_p(\det(A)) < m$, since the valuation, the number of times p divides

pp. 478 for the equivalence of this result between matrices and modules. Now observe that $\mathbb{Z}/p^m\mathbb{Z}$ is a principal ideal ring to get existence and uniqueness of Smith form over this ring. Every ideal in this ring is generated by a power of p and hence the non-zero invariant factors are powers of p .

$\det(A) + p^m q$, is unaffected by the second summand. Taking the valuation of both sides, we then have

$$v_p(\det(A) + p^m q) = v_p(\det(A)) = v_p(\det(L)) + v_p(\det(S)) + v_p(\det(R)).$$

Since $0 \leq v_p(\det A) = v_p(\det S) < m$, it must be the case that $v_p(\det(L)) = v_p(\det(R)) = 0$. \square

Lemma 7. *Fix an integer n , a prime p , and integers $0 \leq e_1 \leq \dots \leq e_n$, and let $m > e_1 + \dots + e_n$. Let $S = \text{diag}(p^{e_1}, \dots, p^{e_n})$ and $\mathfrak{S}_S^m \subseteq \mathbb{Z}^{n \times n}$ as in Definition 2. Fix any $A \in \mathfrak{S}_S^m$. Define*

$$P_A = \{(L, R) : L, R \text{ have entries from } [0, p^m) \text{ and } A = (LSR) \bmod p^m\}.$$

Then $|P_A| = |\text{GL}_n(\mathbb{Z}/p^m\mathbb{Z})^2|/|\mathfrak{S}_S^m|$, independent of the choice of A .

Proof. We have chosen $[0, p^m)$ to represent $\mathbb{Z}/p^m\mathbb{Z}$, so any integer matrix from $[0, p^m)^{n \times n}$ has a unique image over $\mathbb{Z}/p^m\mathbb{Z}$ and vice versa. To keep track of the rings we are working on, we use the subscript p^m to denote matrices over the ring $\mathbb{Z}/p^m\mathbb{Z}$. We first show that there is a bijection between P_A and

$$P'_A = \{(L_{p^m}, R_{p^m}) \in \text{GL}_n(\mathbb{Z}/p^m\mathbb{Z})^2 : A_{p^m} \equiv L_{p^m} S_{p^m} R_{p^m} \pmod{p^m}\}.$$

If $(L, R) \in P_A$, and its image over $\mathbb{Z}/p^m\mathbb{Z}$ is (L_{p^m}, R_{p^m}) , then $(L_{p^m}, R_{p^m}) \in \text{GL}_n(\mathbb{Z}/p^m\mathbb{Z})^2$ by Lemma 6. Also, $A = (LSR) \bmod p^m$ implies that $A + p^m Q = LSR$ for some integer matrix Q and so $A_{p^m} \equiv L_{p^m} S_{p^m} R_{p^m} \pmod{p^m}$. Thus $(L_{p^m}, R_{p^m}) \in P'_A$.

Conversely, let $(L_{p^m}, R_{p^m}) \in P'_A$ and their preimages be $L, R \in [0, p^m)^{n \times n}$. The equivalence $A_{p^m} \equiv L_{p^m} S_{p^m} R_{p^m} \pmod{p^m}$ implies

$$A + p^m Q_1 = (L + p^m Q_2)(S + p^m Q_3)(R + p^m Q_4),$$

for some integer matrices Q_1, Q_2, Q_3, Q_4 . This can be simplified to

$$A + p^m Q_5 = LSR,$$

for some integer matrix Q_5 . In other words,

$$A = (LSR) \bmod p^m,$$

and so $(L, R) \in P_A$. Thus there is a bijection between P_A and P'_A .

We now observe that the multiplicative group $\text{GL}_n(\mathbb{Z}/p^m\mathbb{Z})^2$ acts on $(\mathbb{Z}/p^m\mathbb{Z})^{n \times n}$ via left and right multiplication: $(L_{p^m}, R_{p^m}) \in \text{GL}_n(\mathbb{Z}/p^m\mathbb{Z})^2$ acts on $A_{p^m} \in (\mathbb{Z}/p^m\mathbb{Z})^{n \times n}$ to produce $L_{p^m} A_{p^m} R_{p^m} \in (\mathbb{Z}/p^m\mathbb{Z})^{n \times n}$. Then $\text{orbit}(A_{p^m}) = \text{orbit}(S_{p^m})$ under this group action since there exists at least one such L_{p^m}, R_{p^m} with $L_{p^m} A_{p^m} R_{p^m} \equiv S_{p^m} \pmod{p^m}$. Furthermore, the orbit of S_{p^m} corresponds to \mathfrak{S}_S^m : every matrix in \mathfrak{S}_S^m has a natural image over $\mathbb{Z}/p^m\mathbb{Z}$ which can be written as $L_{p^m} S_{p^m} R_{p^m} \pmod{p^m}$ for suitable choice of $L_{p^m}, R_{p^m} \in \text{GL}_n(\mathbb{Z}/p^m\mathbb{Z})$, and conversely every matrix $L_{p^m} S_{p^m} R_{p^m} \pmod{p^m}$ corresponds to a preimage integer matrix in \mathfrak{S}_S^m . Therefore we know $|\text{orbit}(S_{p^m})| = |\mathfrak{S}_S^m|$.

Let $\text{stab}(S_{p^m})$ be the stabilizer of S_{p^m} defined as:

$$\{(L_{p^m}, R_{p^m}) : L_{p^m}, R_{p^m} \in (\mathbb{Z}/p^m\mathbb{Z})^{n \times n}, S_{p^m} \equiv L_{p^m} S_{p^m} R_{p^m} \pmod{p^m}\},$$

and let $A_{p^m} \equiv U_{p^m} S_{p^m} V_{p^m} \pmod{p^m}$ be a Smith decomposition of A_{p^m} , then every pair $(L_{p^m}, R_{p^m}) \in P'_A$ can be mapped to a pair $(U_{p^m}^{-1} L_{p^m}, R_{p^m} V_{p^m}^{-1}) \in \text{stab}(S_{p^m})$. Similarly, every pair $(L_{p^m}, R_{p^m}) \in \text{stab}(S_{p^m})$ can be mapped to a pair $(U_{p^m} L_{p^m}, R_{p^m} V_{p^m}) \in P'_A$. Thus $|P'_A| = |\text{stab}(S_{p^m})|$.

By the orbit-stabilizer theorem (Artin, 1991, Proposition 7.2), we have

$$|\text{orbit}(S_{p^m})| \cdot |\text{stab}(S_{p^m})| = |\text{GL}_n(\mathbb{Z}/p^m\mathbb{Z})^2|.$$

The lemma statement follows because $|\text{orbit}(S_{p^m})| = |\mathfrak{S}_S^m|$, and $|\text{stab}(S_{p^m})| = |P'_A| = |P_A|$. \square

Lemma 8. *Let $\phi \in \mathbb{Z}[x_1, \dots, x_\ell]$ be a non-zero polynomial and $a_1, \dots, a_\ell \in \mathbb{Z}$. Let p be a prime and $m \geq 1$ be an integer. Let $k = v_p(\phi(a_1, \dots, a_\ell))$ and $\bar{k} = v_p(\phi(a_1 \bmod p^m, \dots, a_\ell \bmod p^m))$. Then*

- (i) *If $k < m$ then $\bar{k} = k$.*
- (ii) *If $k \geq m$ then $\bar{k} \geq m$.*
- (iii) *If $k = \infty$ then $\bar{k} \geq m$.*

Proof. Let $\phi(a_1, \dots, a_\ell) = p^k \alpha$ for some $\alpha \in \mathbb{Z}$ and $p \nmid \alpha$. For all $i \in [1, \ell]$, apply the Euclidean division to a_i and p^m to get $a_i = r_i + p^m q_i$ where $p^m \nmid q_i$ and $r_i = a_i \bmod p^m$. Then

$$\phi(r_1 + p^m q_1, \dots, r_\ell + p^m q_\ell) \equiv \phi(r_1, \dots, r_\ell) \pmod{p^m}.$$

(i) If $k < m$ then

$$\phi(r_1 + p^m q_1, \dots, r_\ell + p^m q_\ell) \equiv \phi(r_1, \dots, r_\ell) \equiv p^k \alpha \pmod{p^m}$$

and $\phi(r_1, \dots, r_\ell) = p^k \alpha + p^m u$ for some $u \in \mathbb{Z}$. Now $v_p(p^k \alpha + p^m u) = k$ since $p^m u$ has valuation at least $m > k$. So $\bar{k} = k$.

(ii) If $k \geq m$ then $\phi(r_1 + p^m q_1, \dots, r_\ell + p^m q_\ell) \equiv \phi(r_1, \dots, r_\ell) \equiv 0 \pmod{p^m}$, and $\phi(r_1, \dots, r_\ell) = p^{m+j} u_1$ for some $u_1 \in \mathbb{Z}$, $p \nmid u_1$ and some $j \geq 0$. Then $\bar{k} = m + j \geq m$.

(iii) If $k = \infty$ then $\phi(r_1 + p^m q_1, \dots, r_\ell + p^m q_\ell) = 0$, and $\phi(r_1, \dots, r_\ell) \equiv \phi(r_1 + p^m q_1, \dots, r_\ell + p^m q_\ell) \equiv 0 \pmod{p^m}$, which is similar to part (ii). \square

Lemma 9. *Let $\phi_1, \dots, \phi_r \in \mathbb{Z}[x_1, \dots, x_\ell]$ be polynomials such that*

$$v_p\left(\gcd\{\phi_1(a_1, \dots, a_\ell), \dots, \phi_r(a_1, \dots, a_\ell)\}\right) = k < m.$$

Then

$$v_p\left(\gcd\{\phi_1(a_1 \bmod p^m, \dots, a_\ell \bmod p^m), \dots, \phi_r(a_1 \bmod p^m, \dots, a_\ell \bmod p^m)\}\right) = k.$$

Proof. There exists an $i \in [1, r]$ such that $v_p(\phi_i(a_1, \dots, a_\ell)) = k$ whereas for all other $j \in [1, r] \setminus \{i\}$, we have $v_p(\phi_j(a_1, \dots, a_\ell)) \geq k$ (and possibly ∞). Then, by Lemma 8, $v_p(\phi_i(a_1 \bmod p^m, \dots, a_\ell \bmod p^m)) = k$ while for all j , $v_p(\phi_j(a_1 \bmod p^m, \dots, a_\ell \bmod p^m))$ is either k or m or higher than m (but not lower than k). Thus the valuation of the desired gcd is also k . \square

We now show that if A is non-singular, then the powers of p in the Smith form of A and $A \bmod p^m$ coincide when $m > v_p(\det A)$.

Lemma 10. *Let $A \in \mathbb{Z}^{n \times n}$ be a non-singular matrix, $m > v_p(\det A)$ and $\bar{A} = A \bmod p^m$. Suppose the invariant factors of A and \bar{A} are s_1, \dots, s_n and $\bar{s}_1, \dots, \bar{s}_n$, respectively. Then $v_p(s_i) = v_p(\bar{s}_i)$ for $1 \leq i \leq n$.*

Proof. Let Δ_i and $\bar{\Delta}_i$ be the i th determinantal divisors of A and \bar{A} respectively. We show equivalently that $v_p(\Delta_i) = v_p(\bar{\Delta}_i)$ for $1 \leq i \leq n$. Each Δ_i (resp. $\bar{\Delta}_i$) is the gcd of all $i \times i$ minors of A (resp. \bar{A}), where each such minor is a polynomial in the n^2 entries of A (resp. \bar{A}). Then by Lemma 9 we have $v_p(\Delta_i) = v_p(\bar{\Delta}_i)$ for all $i \in [1, n]$. \square

Lemma 11. *Let $A \in \mathbb{Z}^{n \times n}$, $\det A \neq 0$ and $m > v_p(\det A)$. Let f_i^M denote the x^{n-i} coefficient of the characteristic polynomial of a matrix M . For all $i \in [1, n]$, if $v_p(f_i^A) = k < m$ then $v_p(f_i^{A \bmod p^m}) = k$.*

Proof. Each f_i^A is the sum of all $i \times i$ *principal* minors of A , which is a polynomial in the entries of A . The claim then follows by Lemma 8. \square

We now apply the above lemmas to get the following.

Lemma 12. *Let A be a p -characterized non-singular matrix and let $m > v_p(\det A)$. Then $\overline{A} = A \bmod p^m$ is also p -characterized.*

Proof. Let Δ_i and $\overline{\Delta}_i$ be the i th determinantal divisors of A and \overline{A} respectively, for $1 \leq i \leq n$. If A is a p -characterized, then $v_p(f_i^A) = v_p(\Delta_i)$ for each $i \in [1, n]$. By Lemma 10 and Lemma 11, we have $v_p(\overline{\Delta}_i) = v_p(\Delta_i)$ and $v_p(f_i^{\overline{A}}) = v_p(f_i^A)$. So \overline{A} is p -characterized. \square

Example 5. *For a prime p consider the matrix A with its Smith form decomposition:*

$$A = \begin{bmatrix} p^3 + 1 & p \\ 2p^4 & p^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -p^4 & 1 \end{bmatrix} \begin{bmatrix} 1 & \\ & -p^2 + p^5 \end{bmatrix} \begin{bmatrix} 1 & p \\ -p^2 & -1 - p^3 \end{bmatrix}$$

whose characteristic polynomial is

$$f = x^2 - (1 + p^2 + p^3)x + p^2 - p^5.$$

Observe that A is p -characterized. Now let $m = 3$ and consider $A \bmod p^m$ and its Smith form decomposition:

$$A \bmod p^3 = \begin{bmatrix} 1 & p \\ 0 & p^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & \\ & p^2 \end{bmatrix} \begin{bmatrix} 1 & -p \\ 0 & 1 \end{bmatrix},$$

which has the characteristic polynomial

$$x^2 - (1 + p^2)x + p^2.$$

Thus $A \bmod p^3$ is p -characterized as well. \square

The following bound is a relatively well-known fact, but we prove it for completeness. Here $M_n(\mathbb{Z}/p^m\mathbb{Z})$ is the ring of $n \times n$ matrices over $\mathbb{Z}/p^m\mathbb{Z}$.

Lemma 13. $|M_n(\mathbb{Z}/p^m\mathbb{Z})|/|\mathrm{GL}_n(\mathbb{Z}/p^m\mathbb{Z})| < 4$.

Proof. Any matrix $A \in M_n(\mathbb{Z}/p^m\mathbb{Z})$ can be written as $A = A_0 + pA_1 + \dots + p^{m-1}A_{m-1}$ with A_i 's having entries from $[0, p)$. Then $A \in \text{GL}_n(\mathbb{Z}/p^m\mathbb{Z})$ if and only if $A_0 \in \text{GL}_n(\mathbb{Z}/p\mathbb{Z})$. There are $(p^{n^2})^{m-1}$ ways to construct the components A_1, \dots, A_{m-1} for each given $A_0 \in \text{GL}_n(\mathbb{Z}/p\mathbb{Z})$. So $|\text{GL}_n(\mathbb{Z}/p^m\mathbb{Z})| = p^{(m-1)n^2} \cdot |\text{GL}_n(\mathbb{Z}/p\mathbb{Z})|$. Next, recall the well-known density bound for non-singular matrices over finite fields:

$$\frac{|\text{GL}_n(\mathbb{Z}/p\mathbb{Z})|}{p^{n^2}} = \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{p^2}\right) \cdots \left(1 - \frac{1}{p^n}\right) > 1/4.$$

Thus

$$\frac{|M_n(\mathbb{Z}/p^m\mathbb{Z})|}{|\text{GL}_n(\mathbb{Z}/p^m\mathbb{Z})|} = \frac{p^{mn^2}}{p^{(m-1)n^2} |\text{GL}_n(\mathbb{Z}/p\mathbb{Z})|} = \frac{p^{n^2}}{|\text{GL}_n(\mathbb{Z}/p\mathbb{Z})|} < 4.$$

□

We can now establish our main density result.

Theorem 2. *Let n be a positive integer, $\epsilon > 0$, and p any prime greater than $16(n^2 + 3n)/\epsilon$. Fix a set of integers $0 \leq e_1 \leq e_2 \leq \dots \leq e_n < \infty$ and let $m \geq e_1 + \dots + e_n + 1$ and $S = \text{diag}(p^{e_1}, \dots, p^{e_n}) \in \mathbb{Z}^{n \times n}$. Then the number of matrices in \mathfrak{S}_S^m which are p -characterized and hence p -correspondent is at least $(1 - \epsilon) \cdot |\mathfrak{S}_S^m|$.*

Proof. Let

$$P = \{(L, R) : L, R \in [0, p^m)^{n \times n}\}.$$

For any $A \in \mathfrak{S}_S^m$, let $P_A \subseteq P$ be as in Lemma 7:

$$P_A = \{(L, R) : L, R \text{ have entries from } [0, p^m) \text{ and } A = (LSR) \text{ rem } p^m\}.$$

If at least one pair $(L, R) \in P_A$ is such that LSR is p -characterized, then A is p -characterized by Lemma 12 (recall $A = (LSR) \text{ rem } p^m$ and $m \geq e_1 + \dots + e_n + 1$ implies $m > v_p(\det A)$). On the other hand, if every pair $(L, R) \in P_A$ is such that LSR is not p -characterized then A can be either p -characterized or not (because the converse of Lemma 12 is not necessarily true; some non p -characterized matrices can become p -characterized after applying $\text{rem } p^m$). To derive an upper bound on the number of non p -characterized matrices in \mathfrak{S}_S^m , we allow the worst outcome: $A = (LSR) \text{ rem } p^m$ is not p -characterized when LSR is not p -characterized for all pairs $(L, R) \in P_A$.

The number of sets, P_A , having every pair (L, R) with a non p -characterized product LSR , can be obtained as the ratio between the total number of pairs giving non p -characterized products (which is at most $(\epsilon/16)|P|$ by Lemma 5) divided by the size of each P_A (which is $|\mathrm{GL}_n(\mathbb{Z}/p^m\mathbb{Z})^2|/|\mathfrak{S}_S^m|$ by Lemma 7). So the maximum number of matrices in \mathfrak{S}_S^m which are not p -characterized is

$$\frac{(\epsilon/16)|P|}{|P_A|} = \frac{(\epsilon/16)|\mathrm{M}_n(\mathbb{Z}/p^m\mathbb{Z})|^2}{|\mathrm{GL}_n(\mathbb{Z}/p^m\mathbb{Z})^2|/|\mathfrak{S}_S^m|} < \epsilon|\mathfrak{S}_S^m|,$$

where the inequality follows using Lemma 13.

Hence there are at least $(1-\epsilon)|\mathfrak{S}_S^m|$ matrices in \mathfrak{S}_S^m which are p -characterized, and each one of those matrices is also p -correspondent by Theorem 1. \square

3.2 Density at small primes

The density estimate of Theorem 2 is limited to large primes. Hereby we report on experiments with small primes. For a given size n and a prime power p^m , we enumerate the set of all $n \times n$ matrices with entries from $[0, p^m)$ and $v_p(\text{determinant}) < m$. We then count the fraction of matrices which are p -correspondent.

Table 1 shows the density of p -characterized and p -correspondent non-singular matrices for small values of p, m, n . The fourth and fifth columns report the fraction (in percentage) of p -characterized and p -correspondent matrices among all $n \times n$ non-singular matrices with entries $[0, p^m)$ and who determinant has p -adic valuation smaller than m . Recall from Example 3 that matrices can be p -correspondent but not necessarily p -characterized, thus the reported p -characterized density is lower than p -correspondent density.

The sixth column in the table reports the minimum percentage of p -characterized matrices among all Smith forms. Given p^m and n , we consider the set of all $n \times n$ matrices with entries $[0, p^m)$ and $v_p(\text{determinant}) < m$. We partition these matrices by their Smith forms localized at p , where we only care about the powers of p in the invariant factors and treat the other prime powers as units. For example, when $p^m = 2^2$ and $n = 2$, we get the following (non-singular) Smith forms localized at 2:

$$\begin{bmatrix} 1 & \\ & 1 \end{bmatrix}, \begin{bmatrix} 1 & \\ & 2 \end{bmatrix}.$$

We then count the fraction of p -characterized matrices in each partition and report the minimum percentage among all partitions.

Table 1: Density (in percentage) of p -characterized and p -correspondent matrices among the set of $n \times n$ non-singular matrices with entries from $[0, p^m)$ and $v_p(\det A) < m$. See the text for an explanation of the last column.

p	m	n	p -characterized	p -correspondent	min p -char.
2	1	2	56.25	81.25	33.33
	2	2	53.52	80.08	33.33
	3	2	53.34	80.00	33.33
	4	2	53.33	80.00	33.33
	1	3	29.10	71.29	18.75
	2	3	26.51	70.14	16.67
	1	4	15.61	66.67	6.667
3	1	2	67.90	90.12	62.50
	2	2	67.50	90.00	50.00
	3	2	67.50	90.00	50.00
	1	3	45.58	86.73	42.77
5	1	2	80.16	96.16	79.17
	2	2	80.13	96.15	78.96
7	1	2	85.76	98.00	85.42

Finally, the table shows that the density drops as n increases and as p decreases, which is consistent with the proofs for large primes. An open and interesting question is to prove similar density estimates for small primes, i.e. when p is small compared to n .

Acknowledgements

The authors are supported by the Natural Sciences and Engineering Research Council of Canada. Computations were carried out using the Sage computer algebra system (Stein et al., 2014). We thank Dino J. Lorenzini and the anonymous referee for providing helpful comments on earlier versions of this paper.

References

- M. Artin. *Algebra*. Featured Titles for Abstract Algebra Series. Prentice Hall, 1991.
- J.-G. Dumas, B. D. Saunders, and G. Villard. On efficient sparse integer matrix Smith normal form computations. *Journal of Symbolic Computation*, 32:71–99, 2001.
- M. Elsheikh, M. Giesbrecht, A. Novocin, and B. D. Saunders. Fast computation of Smith forms of sparse matrices over local rings. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, ISSAC '12, pages 146–153, New York, NY, USA, 2012. ACM.
- L. J. Gerstein. A local approach to matrix equivalence. *Linear Algebra and its Applications*, 16(3):221 – 232, 1977.
- M. Giesbrecht. Fast computation of the Smith form of a sparse integer matrix. *Computational Complexity*, 10(1):41–69, 2001.
- F. Q. Gouvêa. *p-adic Numbers: An Introduction*. Springer-Verlag Berlin, 2nd edition, 1997.
- E. Kaltofen and B. D. Saunders. On Wiedemann’s method of solving sparse linear systems. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC '91)*, volume 539 of *LNCS*, pages 29–38, 1991.
- I. Kaplansky. Elementary divisors and modules. *Transactions of the American Mathematical Society*, 66(2):464–491, 1949.
- T. Kasami, S. Lin, and W. Peterson. New generalizations of the Reed-Muller codes—I: Primitive codes. *IEEE Transactions on Information Theory*, 14(2):189–199, Mar 1968.
- S. Kirkland. Constructably Laplacian integral graphs. *Linear Algebra and its Applications*, 423(1):3–21, 2007.
- N. Koblitz. *p-adic Numbers, p-adic Analysis and Zeta-Functions*. Graduate Texts in Mathematics. Springer-Verlag, 2nd edition, 1984.
- D. Lorenzini. Smith normal form and Laplacians. *Journal of Combinatorial Theory, Series B*, 98(6):1271–1300, 2008.

- M. Newman. *Integral Matrices*. Academic Press, New York, NY, USA, 1972.
- M. Newman and R. C. Thompson. Matrices over rings of algebraic integers. *Linear Algebra and its Applications*, 145:1–20, 1991.
- J. J. Rushanan. Eigenvalues and the Smith normal form. *Linear Algebra and its Applications*, 216:177–184, 1995.
- J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, October 1980.
- W. A. Stein et al. *Sage Mathematics Software (Version 6.2.beta1)*. The Sage Development Team, 2014. <http://www.sagemath.org>.
- J. Wilkening and J. Yu. A local construction of the Smith normal form of a matrix polynomial. *Journal of Symbolic Computation*, 46(1):1–22, January 2011.
- R. Zippel. Probabilistic algorithms for sparse polynomials. In *Symbolic and Algebraic Computation*, volume 72 of *LNCS*, pages 216–226. Springer Berlin, 1979.